eLab Forensics LLC

Cellebrite Reports - 2021 Quick Start User Guide

Pratical Solutions to digital Evidence for Public Defenders

Quick start user guide for opening, navigating and creating custom reports in Cellebrite.

eLab
Forensics LLC

P.O. Box 340355
Hartford, CT 06134

Phone: 877-266-3703
www.elabforensics.com
infor@elabforensics.com

cellebrite mobile forensics fundamentals CMFF
cellebrite certified CCLO logical operator
cellebrite certified CCPA physical analyst
cellebrite certified CCME mobile examiner
cellebrite delivering mobile expertise
WE'RE CERTIFIED.

QUICK START USER GUIDE FOR CELLEBRITE EXTRACTION REPORTS

"For the legal team, by the legal team"

This guide is intended to assist the legal team in managing forensic reports obtained from a cell phone extraction created using Cellebrite.

The purpose of the guide is to create a basic, universal understanding of how to work with these reports. This includes the different levels of extractions, time zone settings, the components that make up an extraction report, the different types extraction report formats, and how to open, view and navigate these reports. In addition, this guide will show you how to search for specific data, create custom reports using the Cellebrite UFED Reader application and what to ask for when requesting reports.

CONTENTS

Introduction……3

Levels of Extraction & Time Zone Settings……3

Report Components……4

PDF Report……5

HTML Report……7

UFDR Report……8

UFDR Report – Search, Filter, Tag and Bookmark……11

Creating Custom Reports……16

Requesting Reports……18

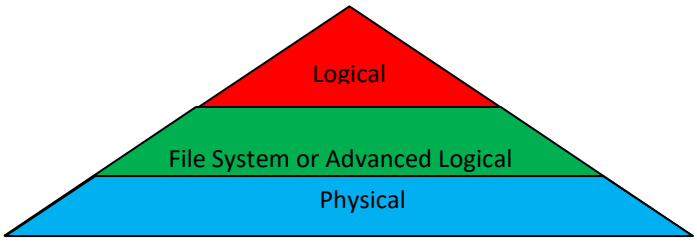
Summary & Hints……19

INTRODUCTION

It is important to know what type of report was provided, what exactly is included and determining what time zone settings was used. This guide will explain the different report formats and how to use them, how different extraction levels can produce more or less results and how to verify the correct time settings.

EXTRACTION LEVELS

Depending on the device, there may be more than one method to extract data and it is not uncommon for more than one extraction to be conducted for the same device. It is important to know the difference between the different extraction levels because each one can recover a different amount of data. However, not all devices are supported for all extraction levels.



Extraction Type	Level	Data Recovered
1. Logical	Basic level	Current data
2. File System	Intermediate level	Current and some deleted
3. Physical	Advanced level	Current data and deleted

A logical extraction obtains the least amount of data. A file system extraction obtains the database files and may recover deleted data still present in the databases. A physical extraction will copy the entire device memory and will recover the most data. The type(s) of extraction conducted will be listed in the *Source Extraction* section of the Cellebrite Report.

TIME ZONES

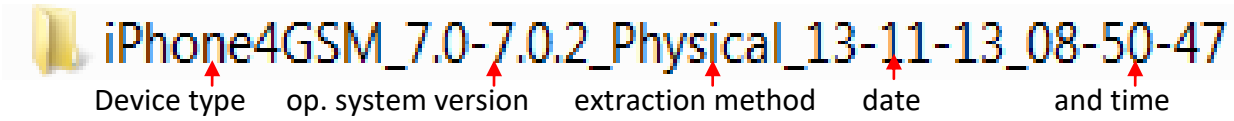
On mobile devices, time stamp information for data items is stored in device memory in coordinated universal time (UTC) and is usually displayed to the device user in local time as obtained from the network. UTC is the primary time standard by which the world regulates clocks and time. UTC represents a vertical line drawn on the earth which crosses Greenwich, England. Time zones around the globe are applied either east or west of this line creating a negative (-) or positive (+) UTC offset. Daylight Saving Time (DST) can also attribute to this time offset based on the time of year.

On the east coast of the United States, Eastern Standard Time would be UTC -5:00 hours and during Daylight Saving Time would be UTC -4:00 hours. On the west coast, UTC -7:00 or UTC -8:00 would be the correct negative (-) offset applied depending on the time of year and whether Daylight Savings Time is observed.

(For more information about setting time zones, see page 9)

REPORT COMPONENTS

A Cellebrite extraction report is usually provided on a disc or USB drive and will have several components which work together. The report will be in a folder that contains files and sub folders. It will usually be labeled by the type of device that was extracted, the device operating system version, type of extraction and the date and time of the extraction, but could vary.



Because of the size of these files it is recommended that the entire folder by copied to your desktop so opening and navigation will be faster.

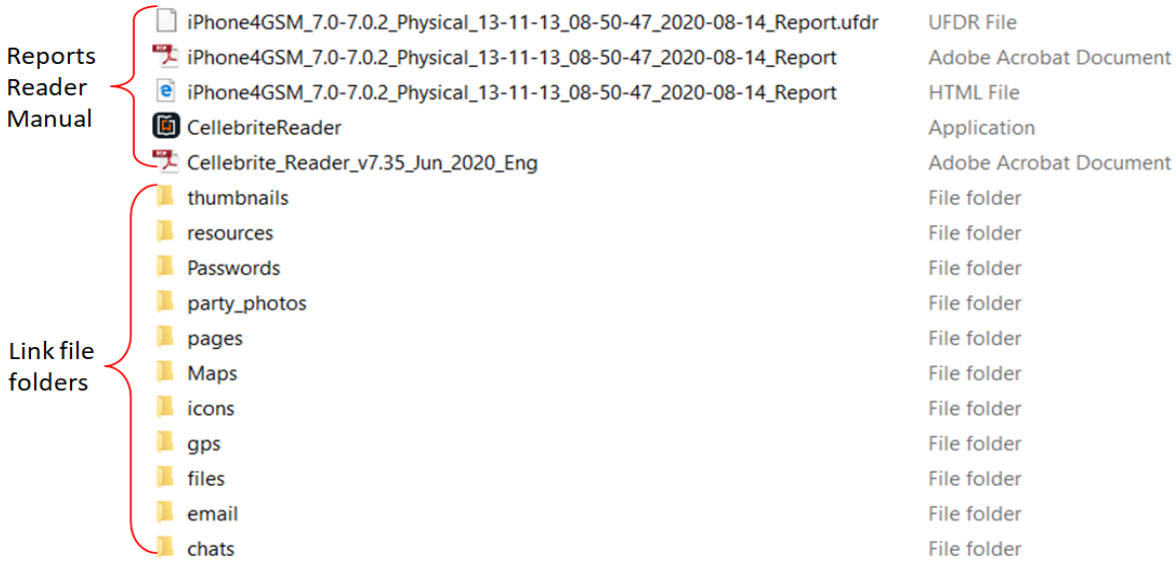
Files & Sub-Folders

The folder may contain extraction reports in more than one format along with associated file folders containing link files. The extraction reports and link file folders need to remain together. The links will not work if both components are not provided or if the file and folders are not together. The three (3) most common Cellebrite report format types are:

1. PDF report (Adobe document report file)
2. HTML report (Web browser)
3. UFDR report (Cellebrite UFED Reader)

Components

The following image shows the contents of the sample report folder with the three (3) different Sample types, PDF, HTML and UFDR and associated link file folders. The folder should also contain a UFED Reader program needed to open the UFDR file and a UFED Reader manual on how to use the program and create custom reports. ***(See page 7 for more information about the UFED Reader)***

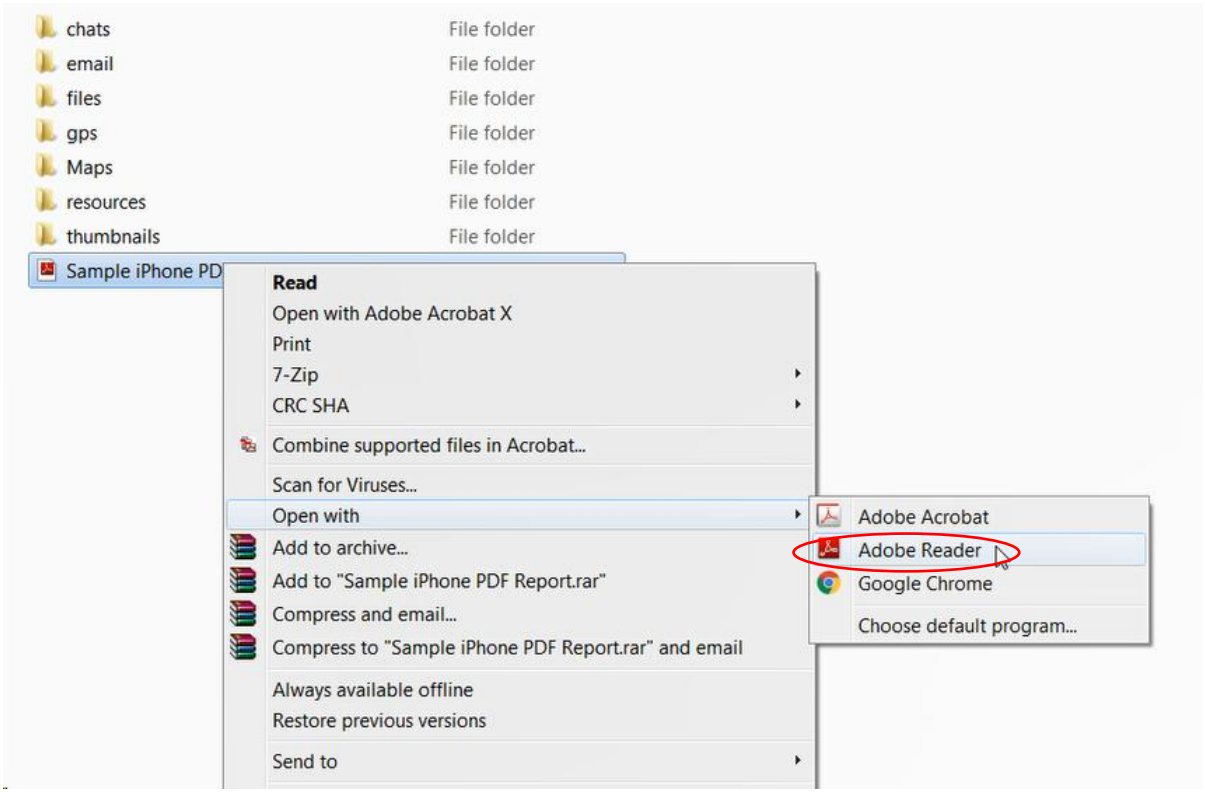


PDF REPORT

A Cellebrite PDF format report can contain links to associated multimedia files such as images, video and audio recordings. The report may display small thumbnail images for photos and videos. Clicking on the hyperlinks will open full-size images or files such as videos or voicemail recordings will be played by the associated program. The actual data is contained in the associated link file folders found on the same file level with the report. These components work together and must be kept in the same folder to work correctly.

Open Using Adobe Reader

The PDF report should be opened using Adobe Reader for the hyperlinks to function properly. Other Adobe programs such as Adobe Acrobat may result in errors when attempting to open the link files. To open the report with Adobe Reader, right click on the PDF report and select: *Open with > Adobe Reader*.



Navigating PDF Reports

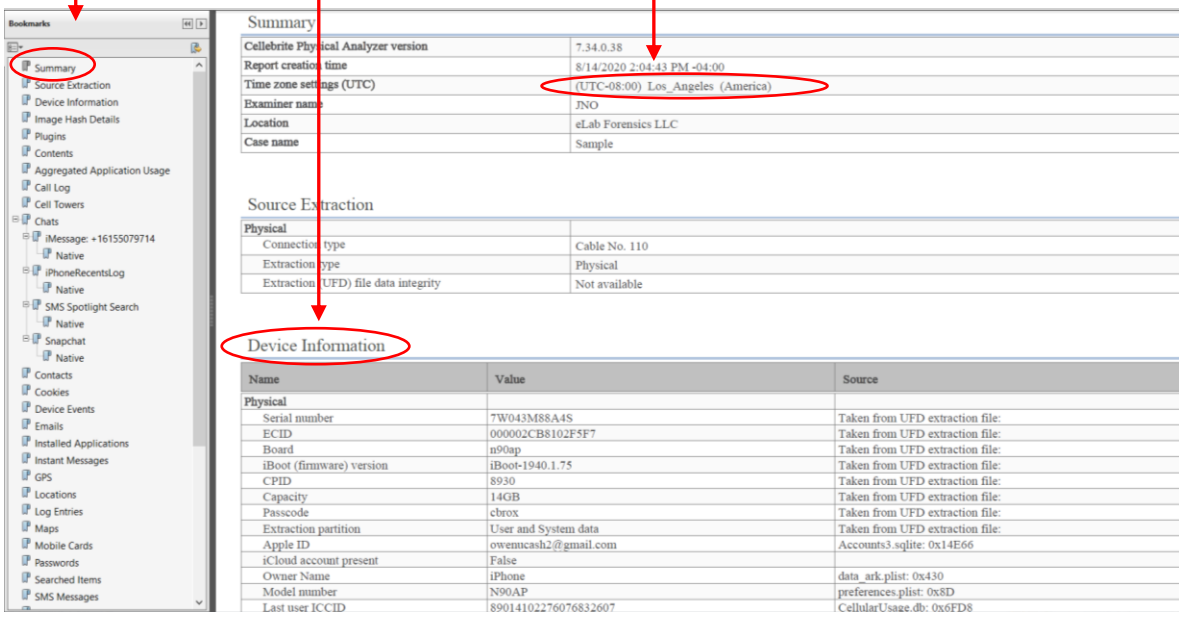
When the PDF report is opened it will display a folder hierarchy structure or index in the left pane and the details will be displayed in the larger pane.

The details about the device extraction, date, type and examiner are in the Summary section located on the first few pages of the PDF report.

The UTC settings are displayed in the summary section.

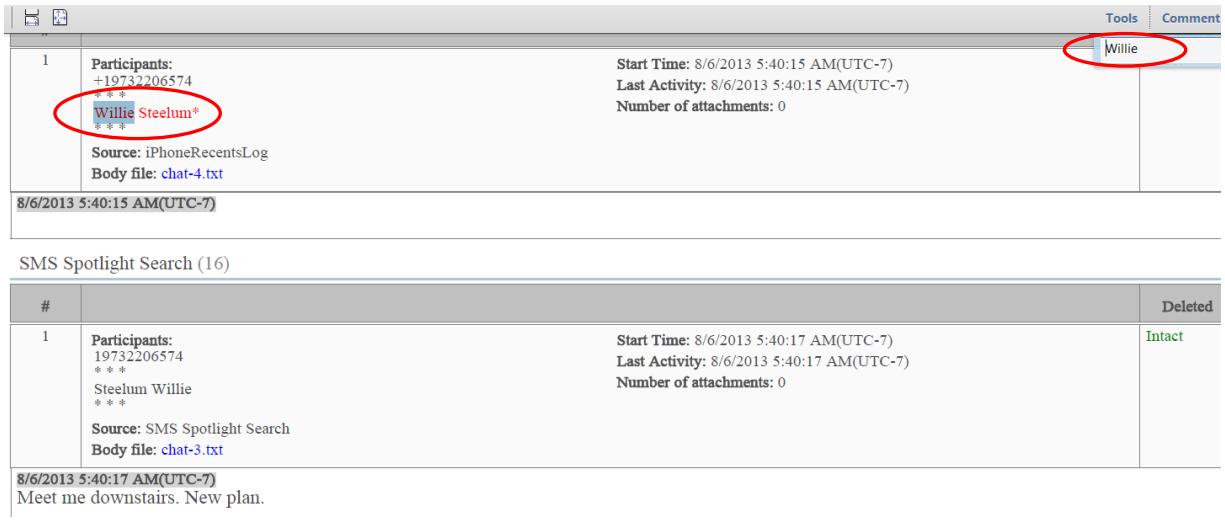
Quick Navigation: Click on the folder in the index to jump to the desired report section.

Folders Index Details Time Zone Settings



Keyword Searches

On the PDF report, searches can be conducted by using the ***Ctrl+f*** function and entering search terms in the dialog box.



HTML REPORT

An HTML (Hypertext Markup Language) style report is made up of a single document broken up into different sections with an index that will open the results in new tabs, displaying like a web page in a web browser. Firefox, Chrome or Microsoft Edge browsers are recommended since Internet Explorer (IE) is no longer supported. If IE is the default viewer, the HTML report can be opened using Chrome or Firefox using the "Open with" procedure described on page 4.

The basic information as to the device information and the extraction details are at the beginning of the report.

The contents section will be at the bottom and will contain an index of links along the left side that can be clicked on to open content areas in different tabs.

Contents

Type	Included in report	Total
Application Usage	8	8
Call Log	13	13
Cell Towers	45	45
Chats	25 (3 Deleted)	25 (3 Deleted)
• iMessage: +16155079714	3 (2 Deleted)	3 (2 Deleted)
• iPhoneRecentsLog	1	1
• SMS Spotlight Search	16 (1 Deleted)	16 (1 Deleted)
• Snapchat	5	5
Contacts	9	9
Cookies	79 (19 Deleted)	79 (19 Deleted)
Emails	111 (31 Deleted)	111 (31 Deleted)
Installed Applications	55	55
Instant Messages	1	1
Locations	318 (45 Deleted)	318 (45 Deleted)
Log Entries	31	31
Maps	1	1
Mobile Cards	1	1
Passwords	27	27
Powering Events	38	38
SMS Messages	35 (4 Deleted)	35 (4 Deleted)
User Accounts	7 (1 Deleted)	7 (1 Deleted)
User Dictionary	44	44

<u>Searching</u>

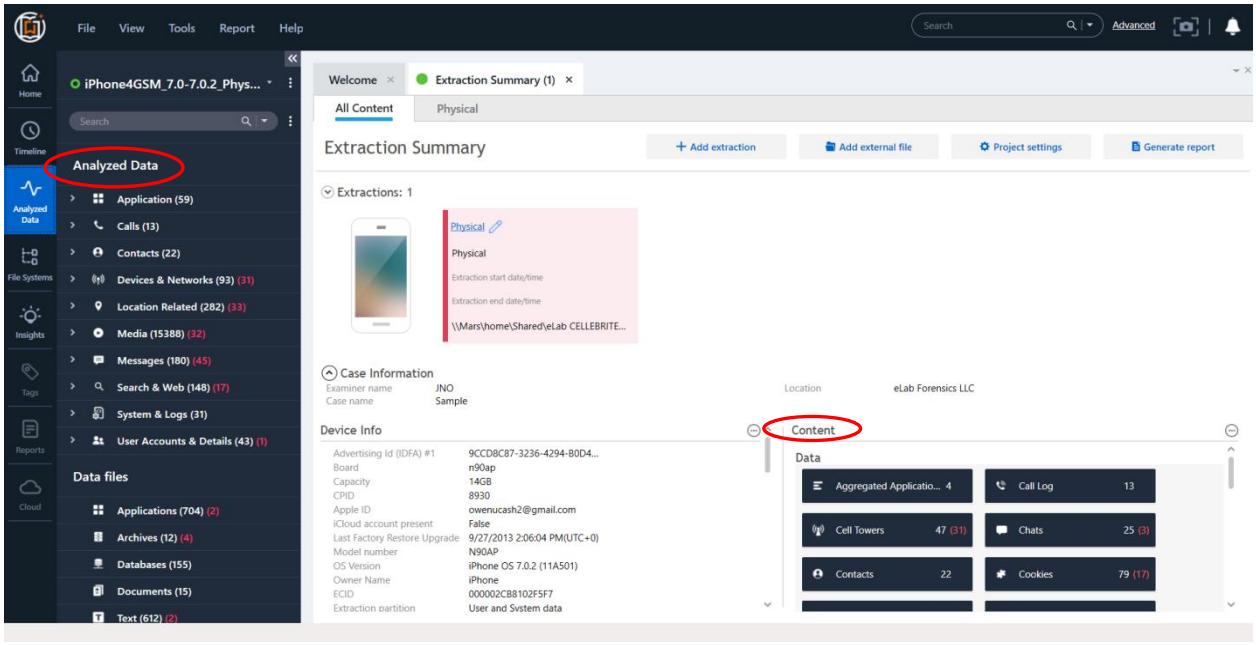
Use the ***Ctrl+f*** function to run keyword searches, but it will only work on the individual page tabs rather than from the main page.

<u>*Note: Opening Link Files</u>

While reviewing reports in HTML format it is important to know that clicking a web site link would automatically open the file from the internet which could contain adult content.

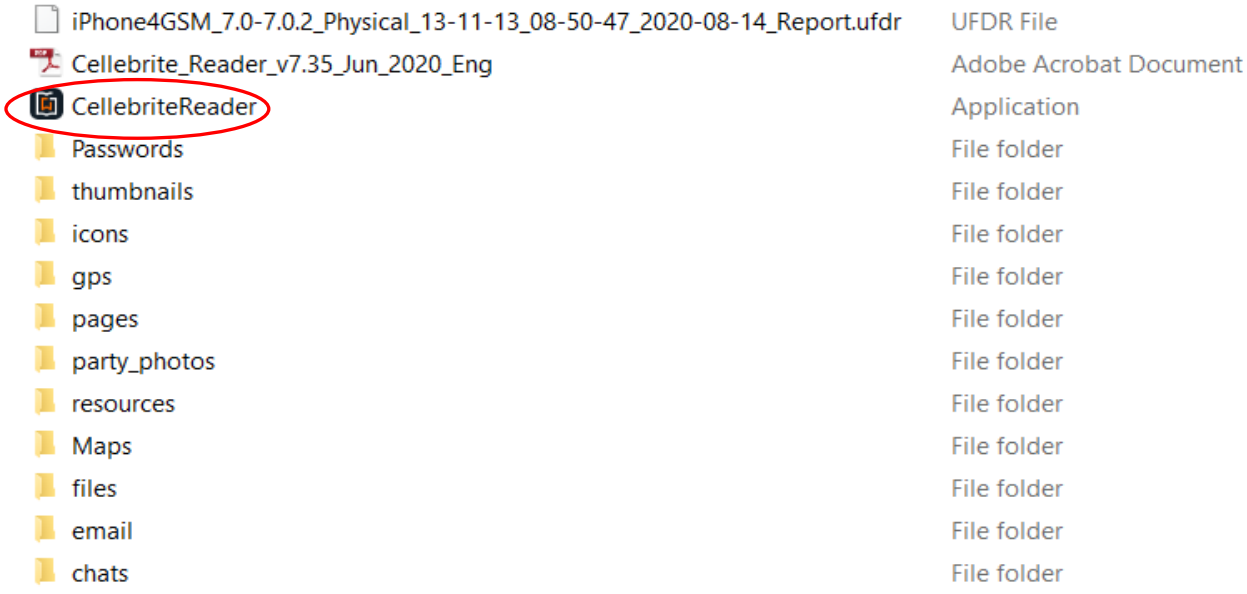
UFDR REPORT

The Cellebrite UFED Reader (UFDR) report is Cellebrite file that allows the user to conduct advanced searches, filtering, timeline queries, tags, bookmarks, and project savings as well as generate customized reports in multiple formats. It requires the Cellebrite UFED Reader program to open that should be included with the extraction. UFDR report allows the most flexibility and will resemble the Cellebrite dashboard the forensic examiner sees during the examination. It has an easy to navigate index along the left side column under analyze data and a quick navigation area under *Content*, all on the main screen. A Cellebrite UFED Reader user manual should also be included.



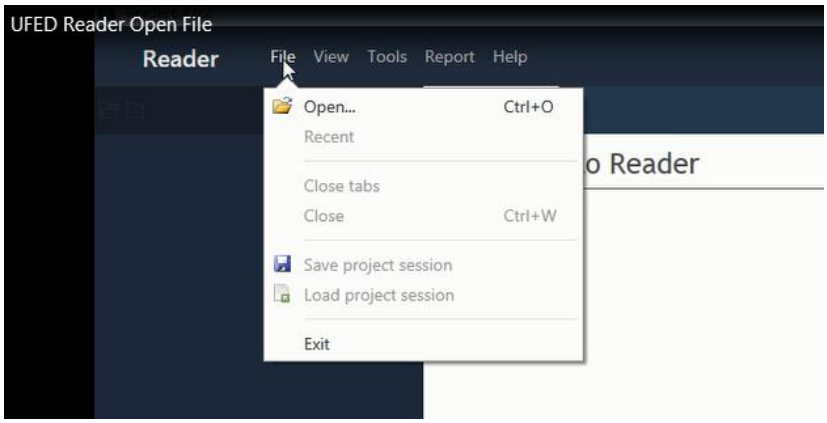
<u>Open Using Cellebrite Reader</u>

Click on CellebriteReader and the associated UFDR report should automatically open the home screen as displayed on page 7.

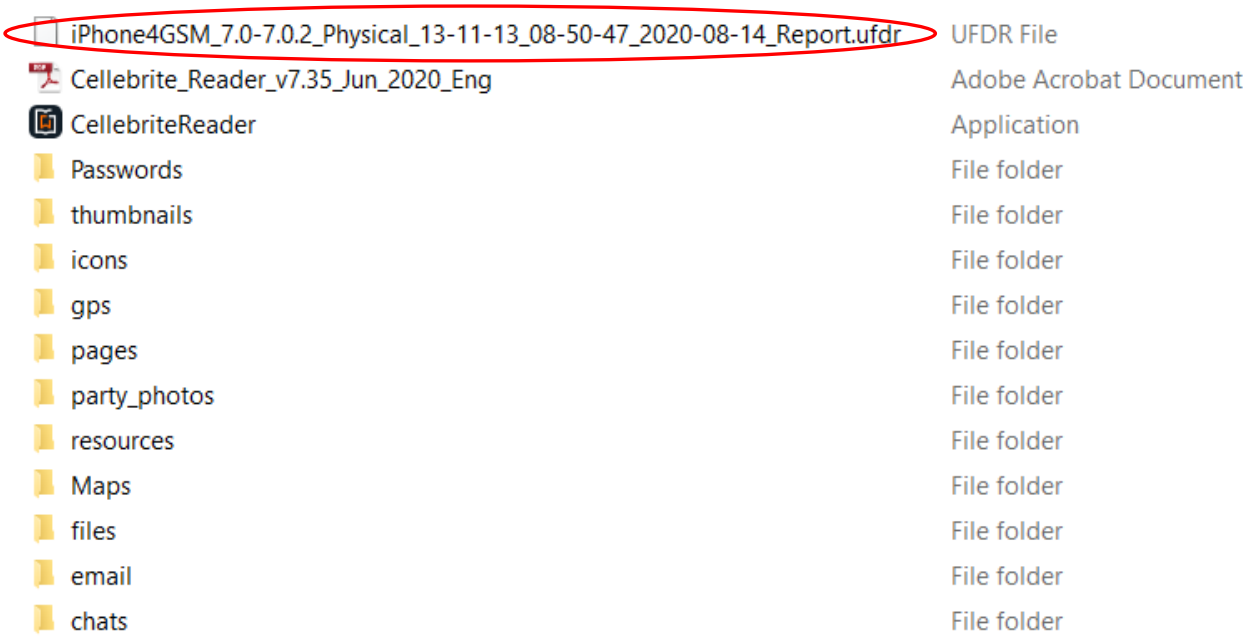


Manually Opening UFDR report with the UFED Reader Program

In some cases, it may be necessary to manually open a UFDR report file with the UFED Reader program. After launching the UFED Reader program application, select *File* > *Open* from the upper left toolbar:

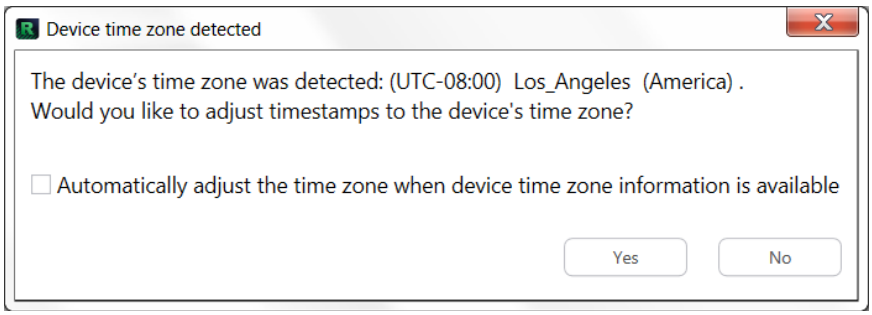


Then navigate to the location of the UFDR Report file to be opened:



Time Zone Settings

Most mobile devices store the last time zone setting used. If present, Cellebrite will detect this information and indicate the time zone used upon opening the report:



It is usually beneficial to set the device to the time zone used to see the data time stamps in the user's local time. One exception could be when multiple devices from different time zones are being examined. By leaving the time settings in UTC, the common items will all display as the same time.

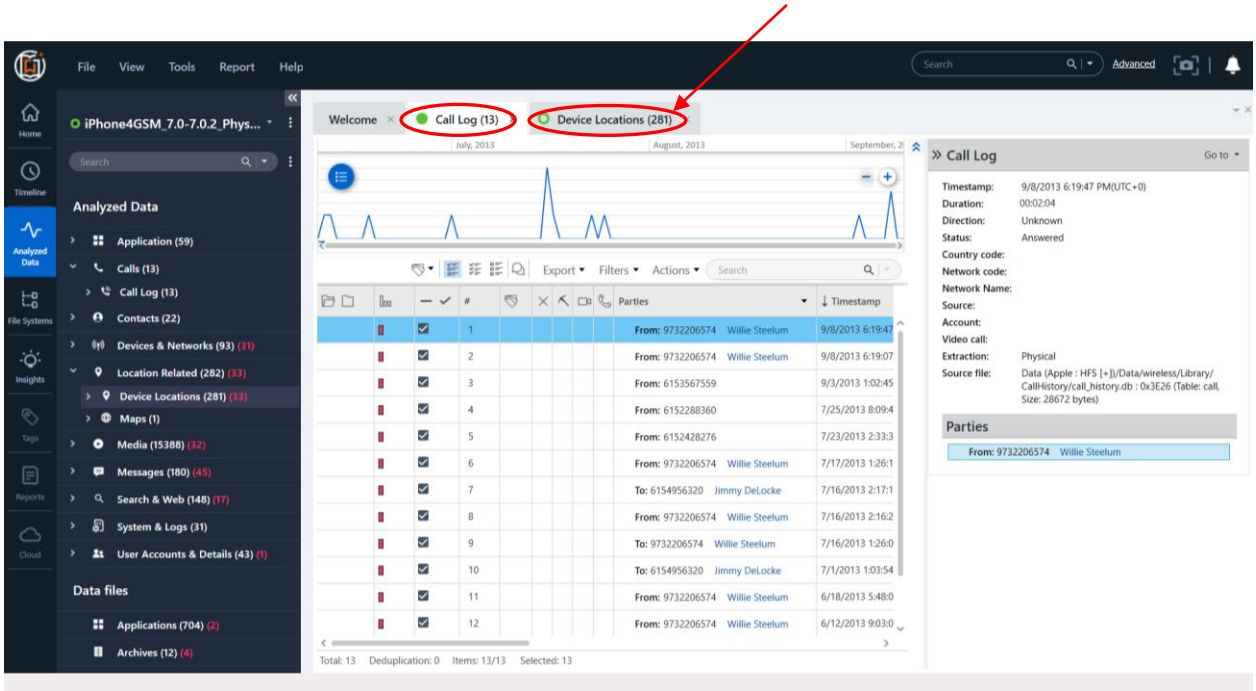
If the time zone was not adjusted to the detected time zone by the examiner or not detected automatically at the time of extraction, the time zone can be set manually from the Project Settings in the upper right of the Extraction Summary tab.

Data Tabs

Data tabs show files of a specific type such as call log, contacts, SMS messages etc.
Data in data tabs display as a sub tab along the top, depending on the type of data:

- Text view - View text files as text.
- Table view - a list of all the files of a specific type.
- Thumbnail view - view images by thumbnail.
- Folder view - view the folder structure of the data files paths.
- Image view - view the image.
- File Info - view information about the file.

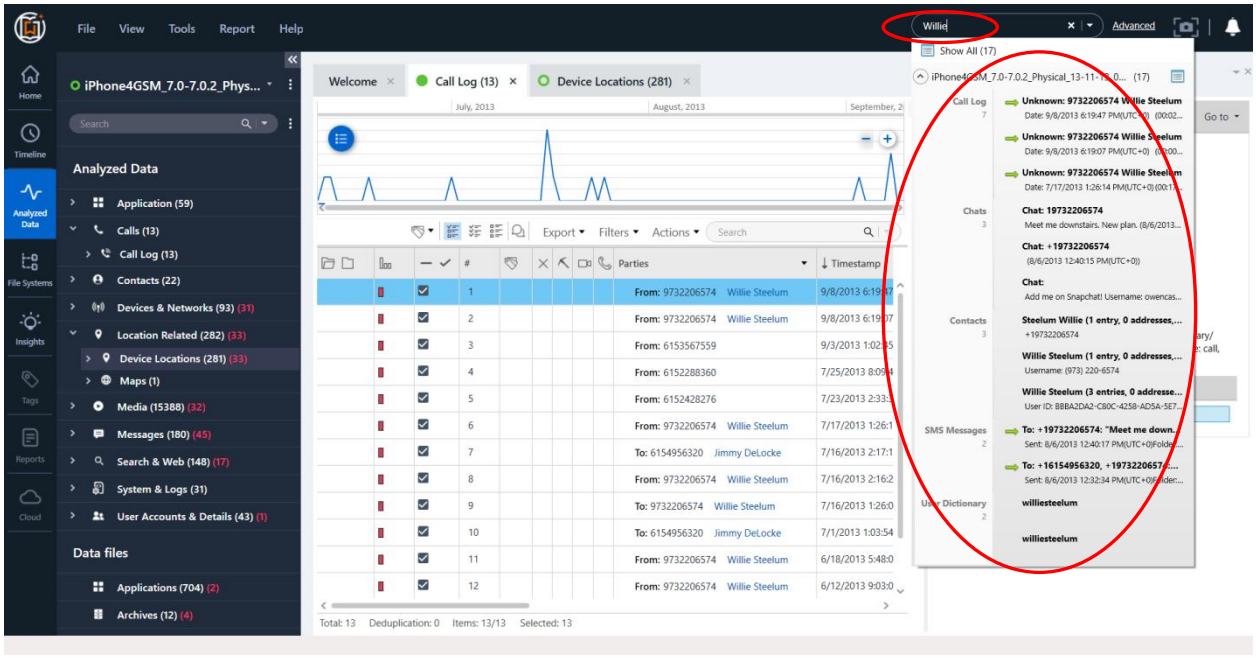
In the following example two sub tabs for Call Log and Device Locations are displayed. The numbers next to the name indicate how many records exist.



UFDR REPORT – SEARCH, FILTER, TAG AND BOOKMARK

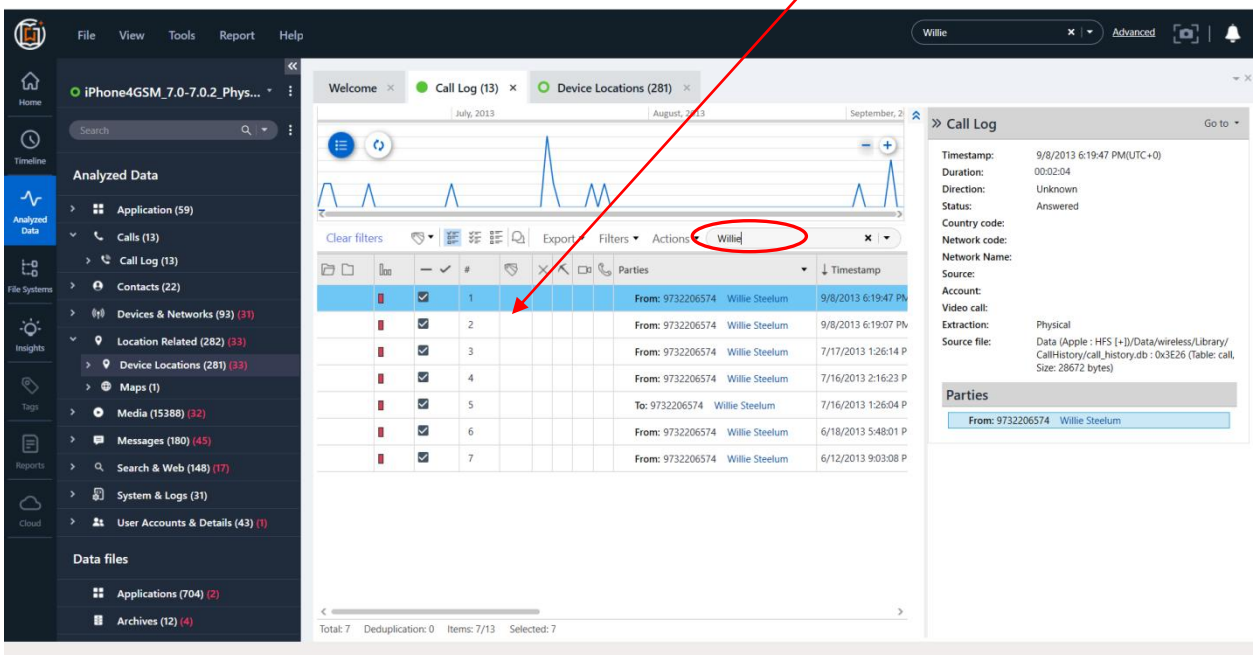
Searching Entire Extraction

To conduct a global search, enter the search term in the search box in the header shown below. This will show all a listing of the results in the data tabs where the search term was located.



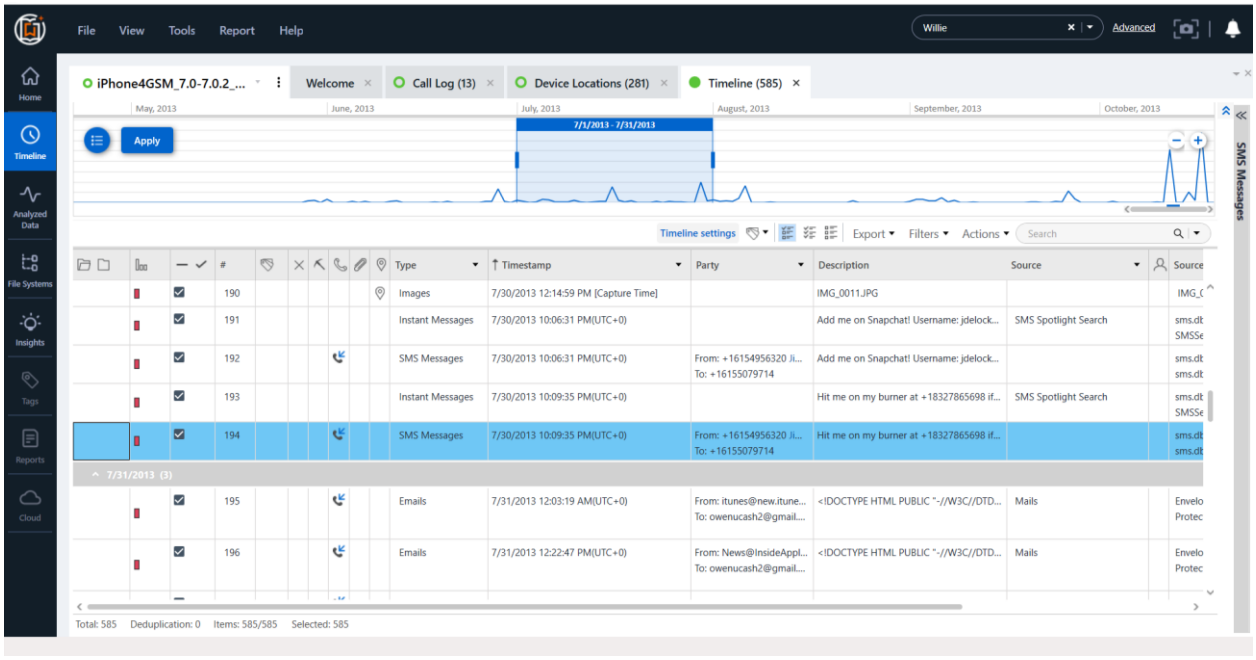
Searching individual data tab

Enter the search term in the search window shown below. The data table updates to display the results of the search.



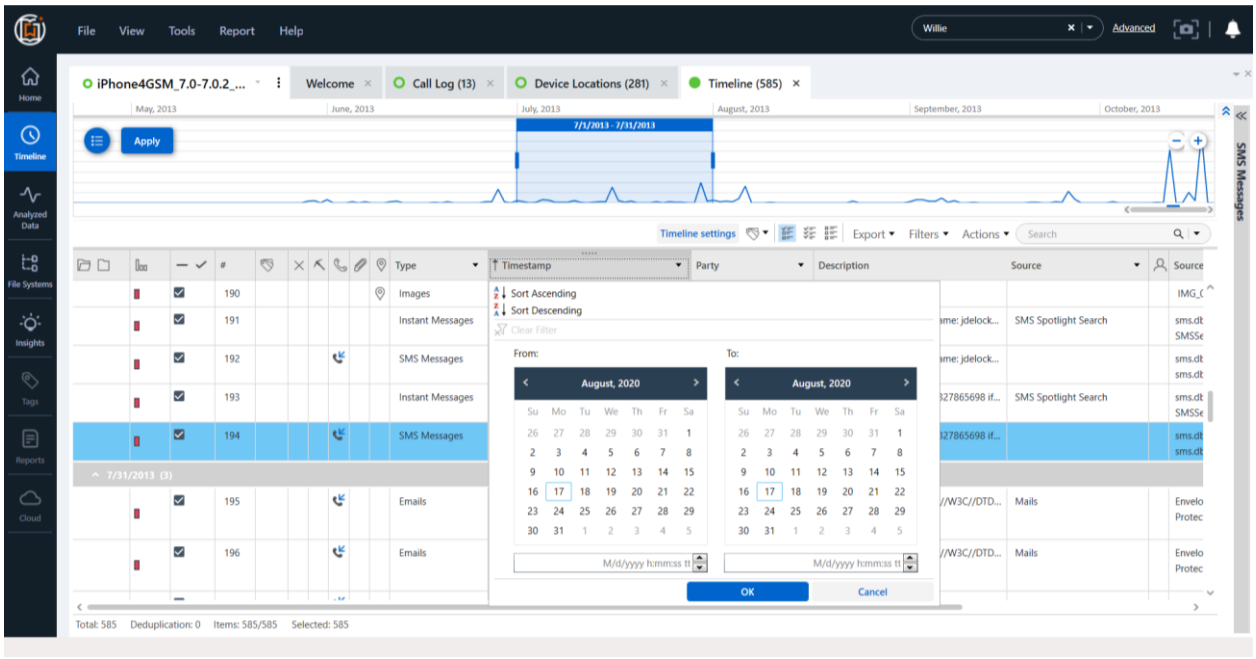
Timeline Search

Timeline view is a powerful tool that enables you to analyze data in chronological order.



Filtering and Sorting

In any Analyzed data or Data file window, the listed results are filtered by column. Click on the relevant column heading to view filter and sort options.

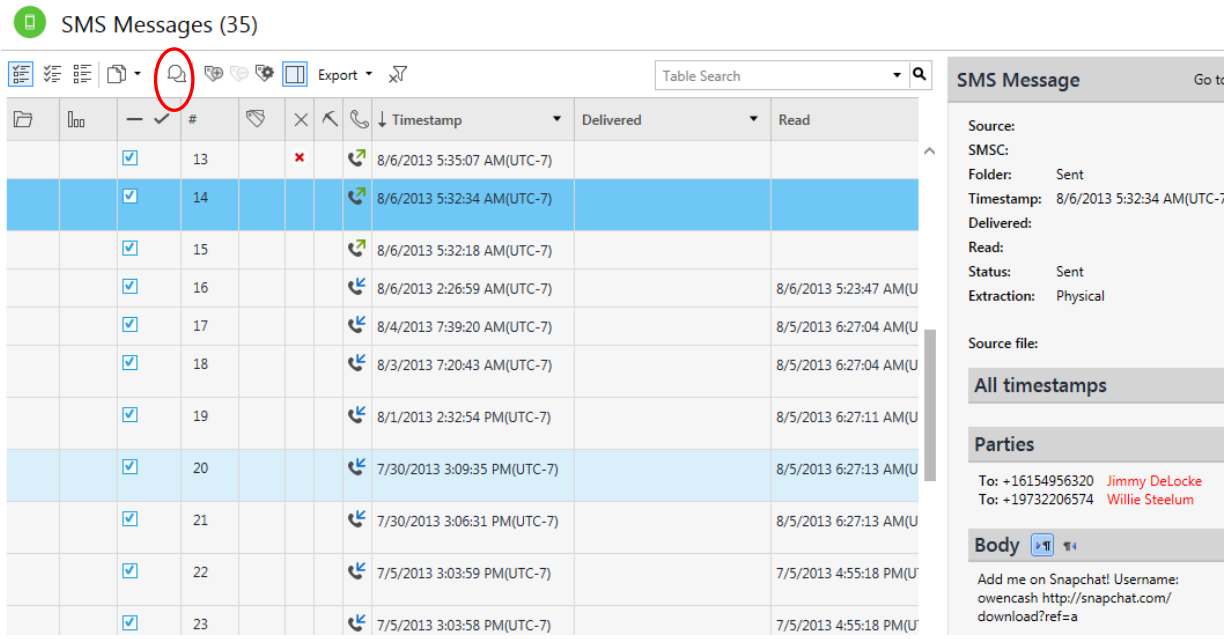


Conversation view

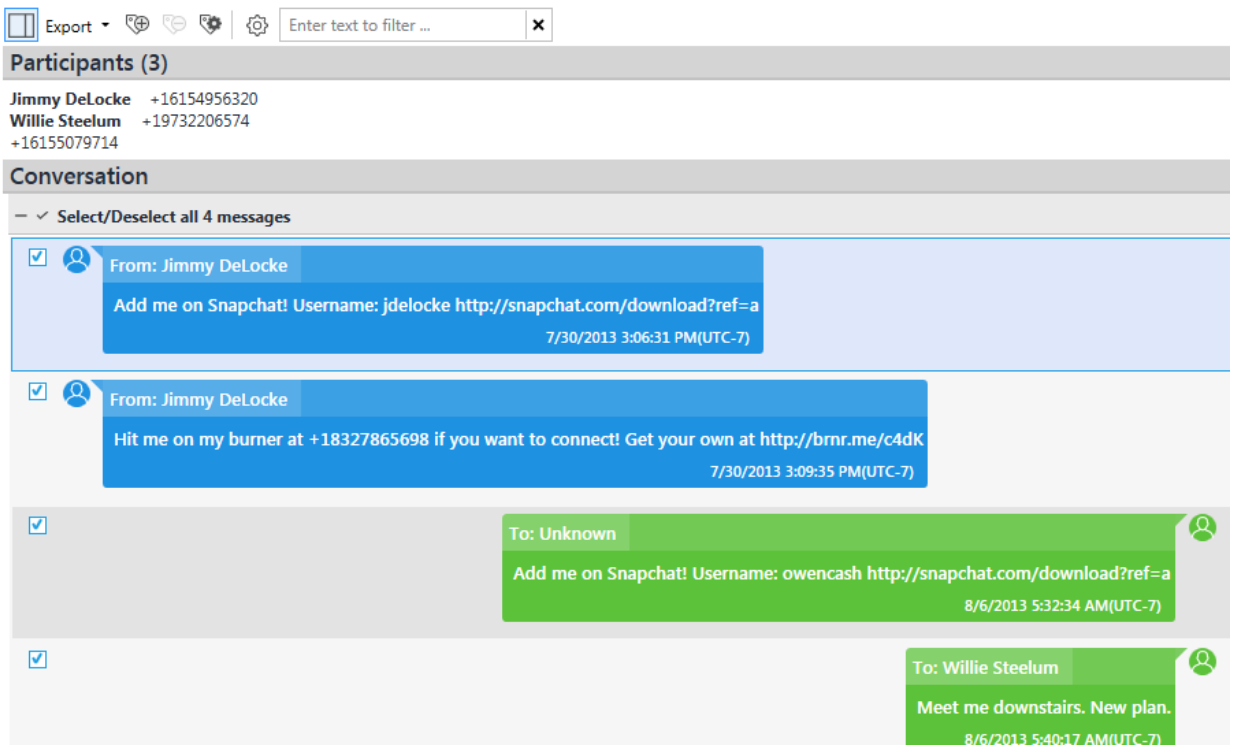
Communication-based data (text messages) can be displayed in a conversation view layout between two or more parties that resemble what the user would see on their device.

Open Conversation View

Use the conversation view button to see all related messages in a threaded view:

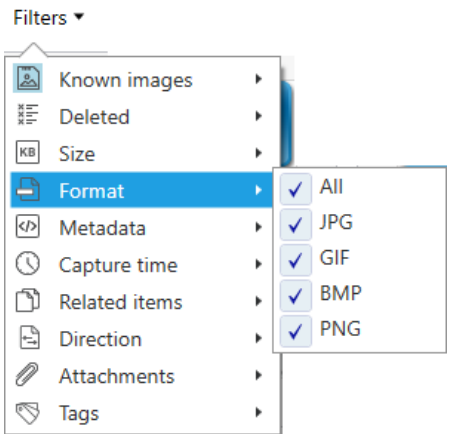


Conversation View Example



Using the Quick Filter

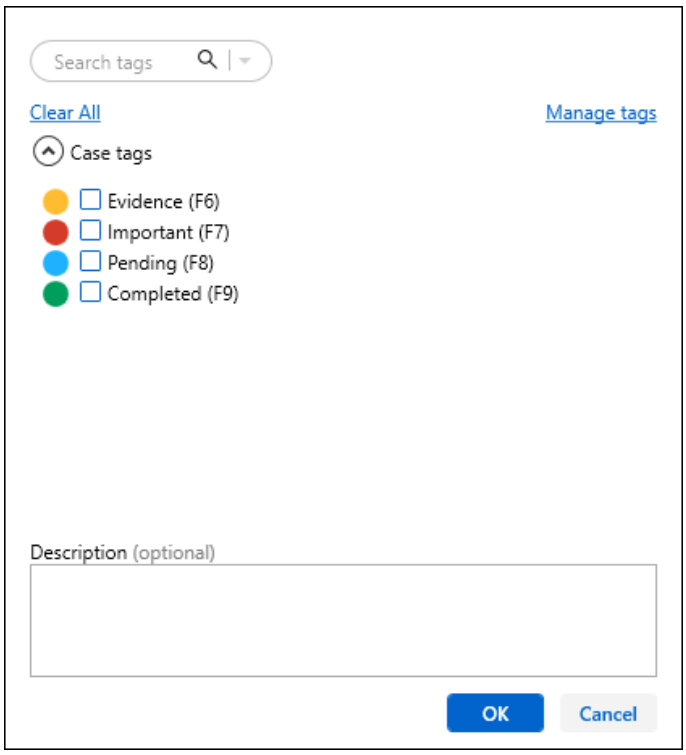
To improve accessibility the filters are now grouped under simple menus.



Tags

The investigator can tag items for future reference and quickly generate a report from tagged items. Each item can have multiple tags. To add a tag to timeline items:

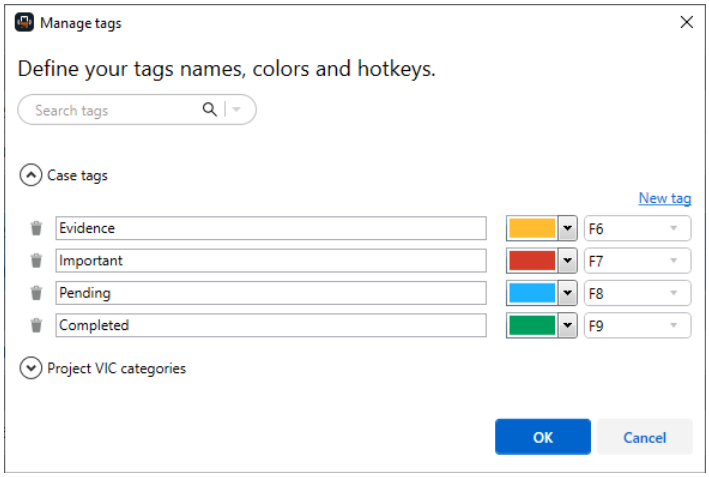
1. Select one or more row in the timeline table.
2. Click .
3. Select Tag.
4. Select the required tags.



5. Click OK.

Manage Tags

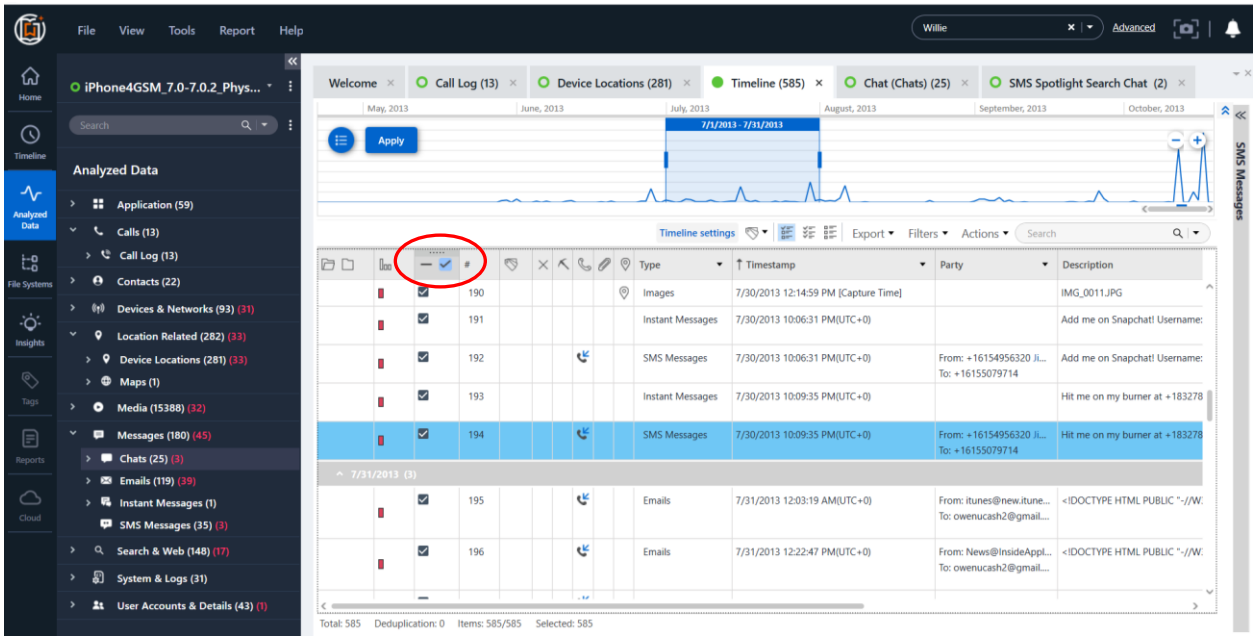
1. Click .
2. Select Manage tags.
3. In the Manage tags window you can:
   - Search tags.
   - Rename existing tags.
   - Delete tags.
   - Define tag color.
   - Define tag hotkey.
   - Create a new tag by clicking New tag.



4. Click Ok.

Bookmarking

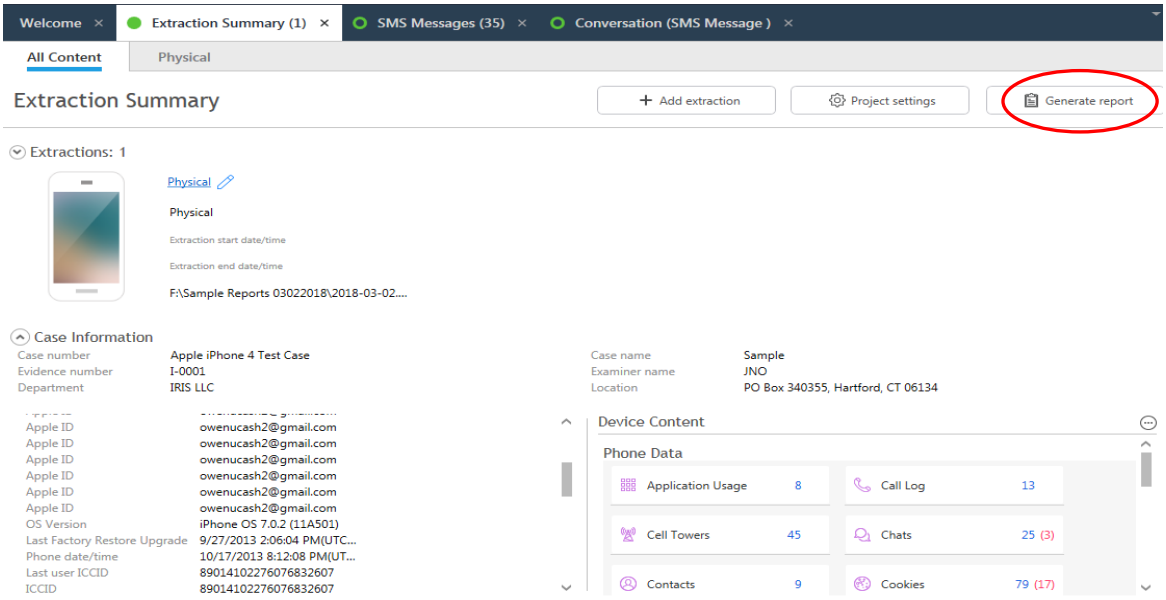
Using the UFED Reader application, any relevant data identified can be bookmarked for inclusion in the report. To include items in a report, the check box next to the data item(s) must be selected as follows:



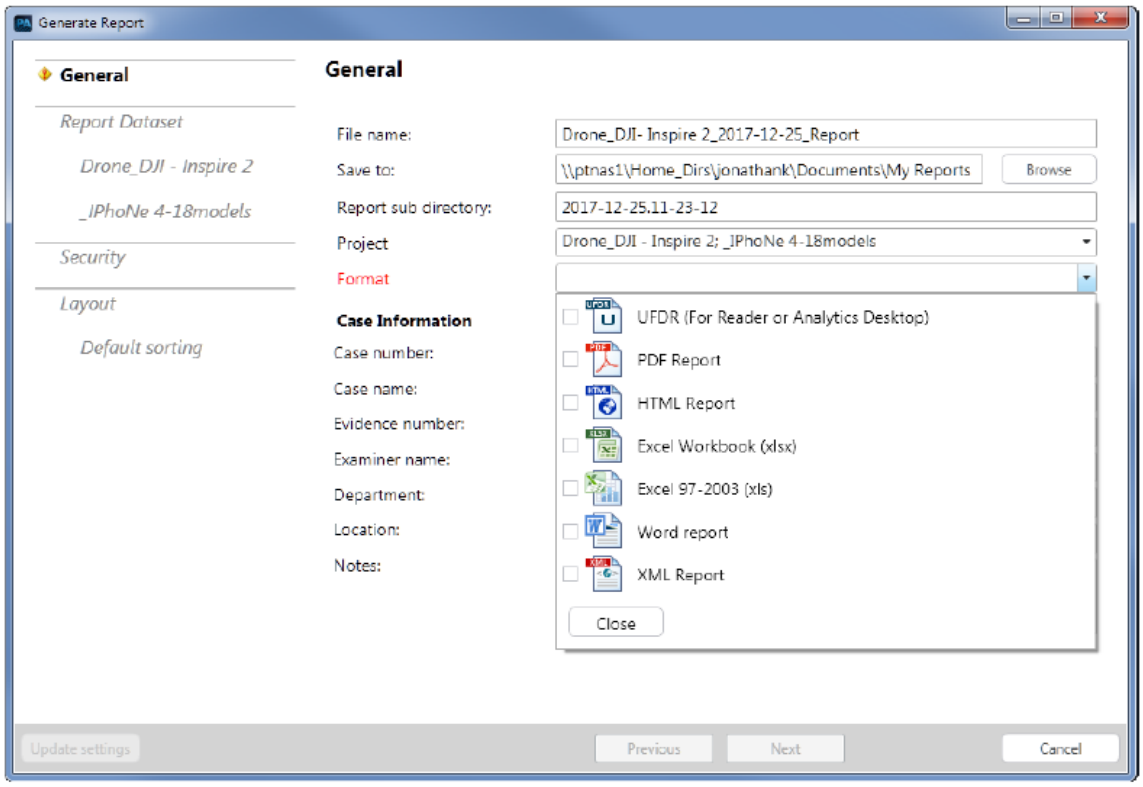
CREATING CUSTOM REPORTS

(See the Cellebrite UFED Reader manual for further information on creating reports)

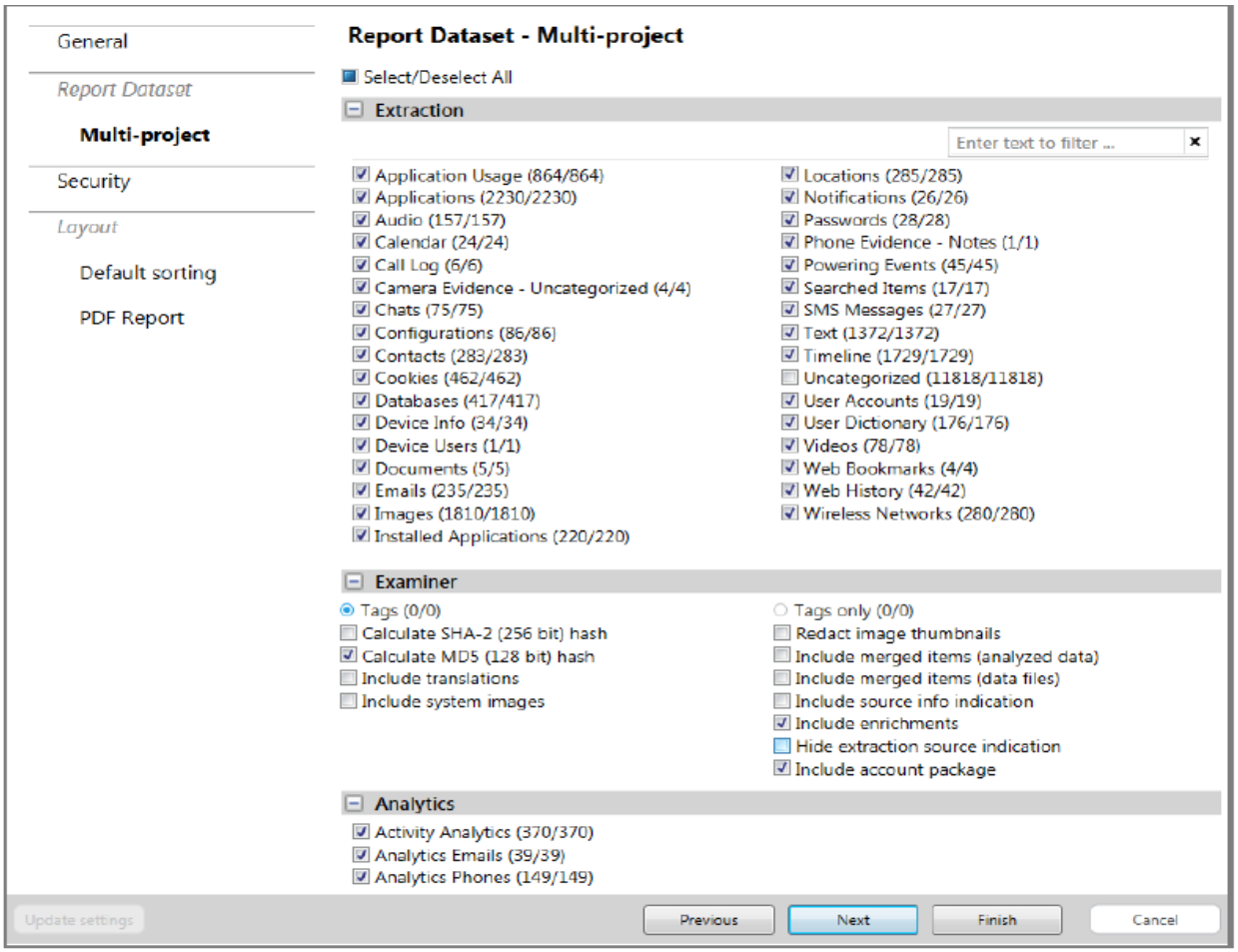
Using the UFED Reader application, any relevant data identified can be bookmarked for inclusion in the report. A new report is created from the Extraction Summary tab:



Select the desired report format(s) and input any case information:

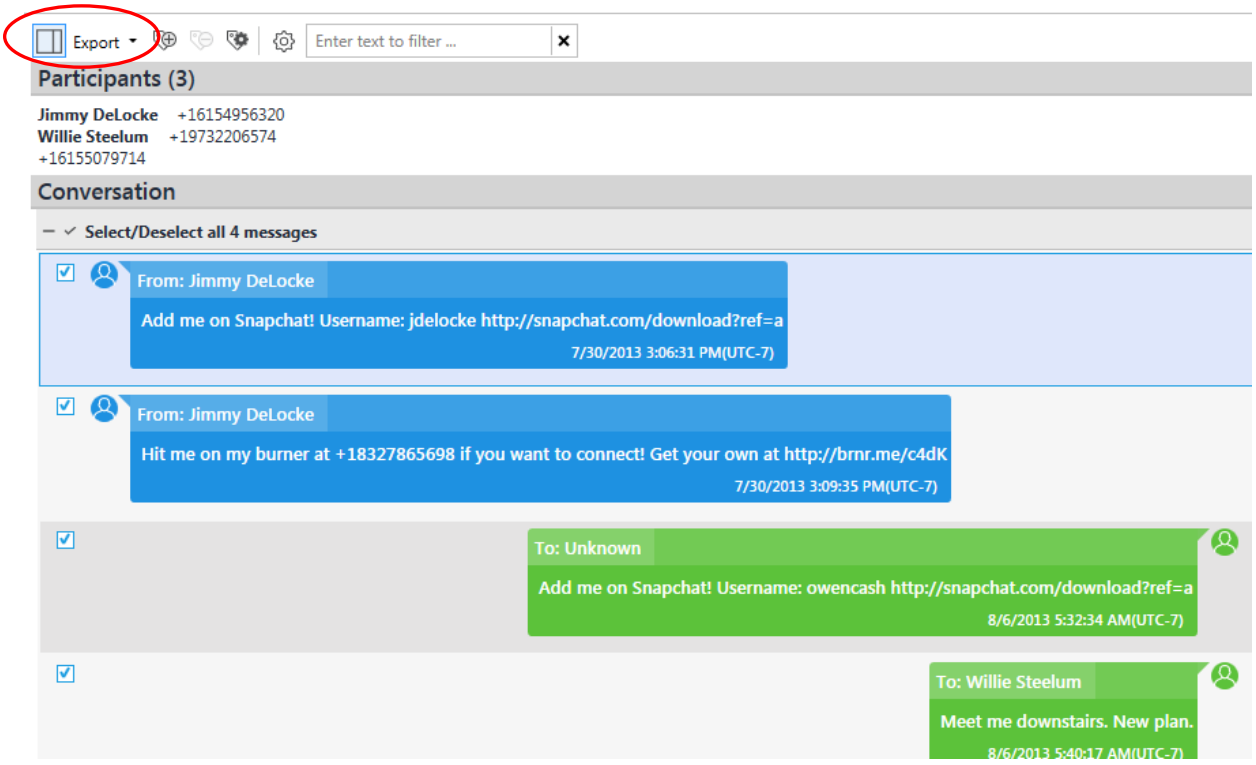


Specific data types can be selected for inclusion in the report:



Export Single Report Items

Use the export drop down box and select the desired output format for individual item reports:



REQUESTING REPORTS

When dealing with digital evidence from a mobile device that has been preserved and examined by law enforcement, industry standards recommend that a full report and copy of the original extraction file and proprietary file viewer be requested.

When requesting Cellebrite reports, the entire extraction should be requested in PDF, HTML and UFDR style formats. The UFED Reader program and manual should be requested as well as the copy of the forensic extraction in the native proprietary format.

Sample Request

1. ***All reports including search warrant or consent, and reports regarding the seizure and the chain of custody of the evidence.***

2. ***The forensic examiners report detailing the tools and all procedures used to examine the device.***

3. ***A copy of the extraction file in the native (original) format of the forensic device or software used to conduct the extraction.***

4. ***Full forensic extraction report in PDF and HTML format.***

5. ***Forensic Report in UFED Reader format with UFED Reader file viewer.***

6. ***The proprietary file viewer for the specific forensic tool used to create the extraction.***

SUMMARY

A logical extraction is fast and easy, but will not recover deleted data.

A physical extraction will get the most data, but could take much longer to run.

Not all devices are supported for all levels of extraction.

The report could be in three (3) different format types.

Save extraction reports to desktop for faster file access.

Be sure you are aware of the time setting that was set for the report.

The PDF Report needs to be opened using Adobe Reader for the link files to work.

HTML link files will open in your internet browser and may bring you to the website visited.

When viewing HTML reports, keyword searches are available only if the tab of the desired area has been opened.

The Cellebrite UFED Reader Program is needed to open UFDR Report.

The links will not work if both the report and associated link file folders are not provided or are not together.

Be sure to request the forensic extraction in its native proprietary format.

HINTS

UTC Time
EST = Eastern Standard Time (UTC - 5 hours), (Autumn/Winter)
EDT = Eastern Daylight Time (UTC - 4 hours) (Spring/Summer)

Rapid assessment
Navigate to the timeline to review activities around the time of incident.

Locating email addresses
Use @ symbol in keyword searches to find email addresses.

Creating Custom Reports
See the UFED manual for further information on generating reports using the UFED Reader.

For More Information
Visit our website at www.elabforensics.com or call us directly **877-266-3703**.

References
www.cellebrite.com